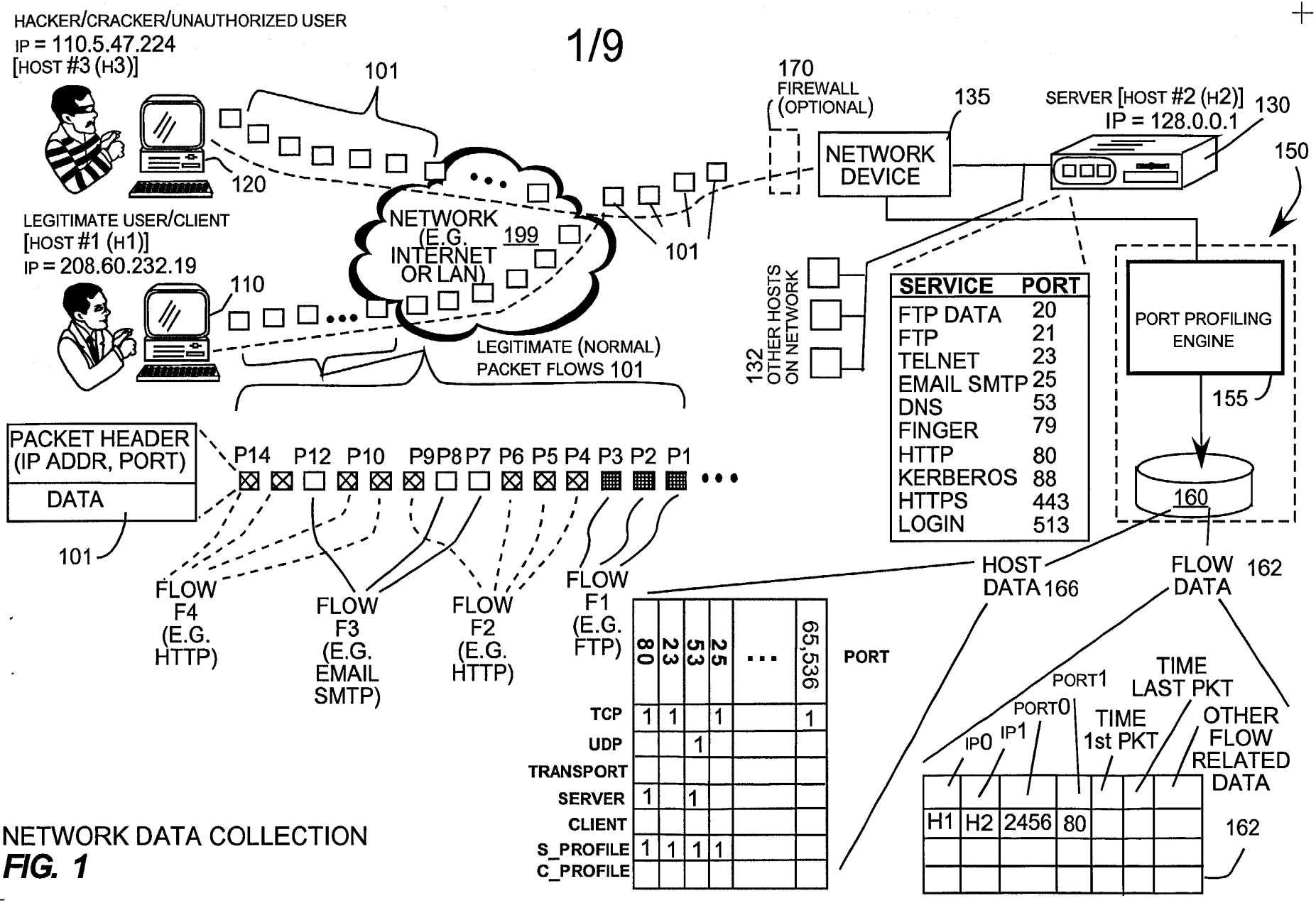
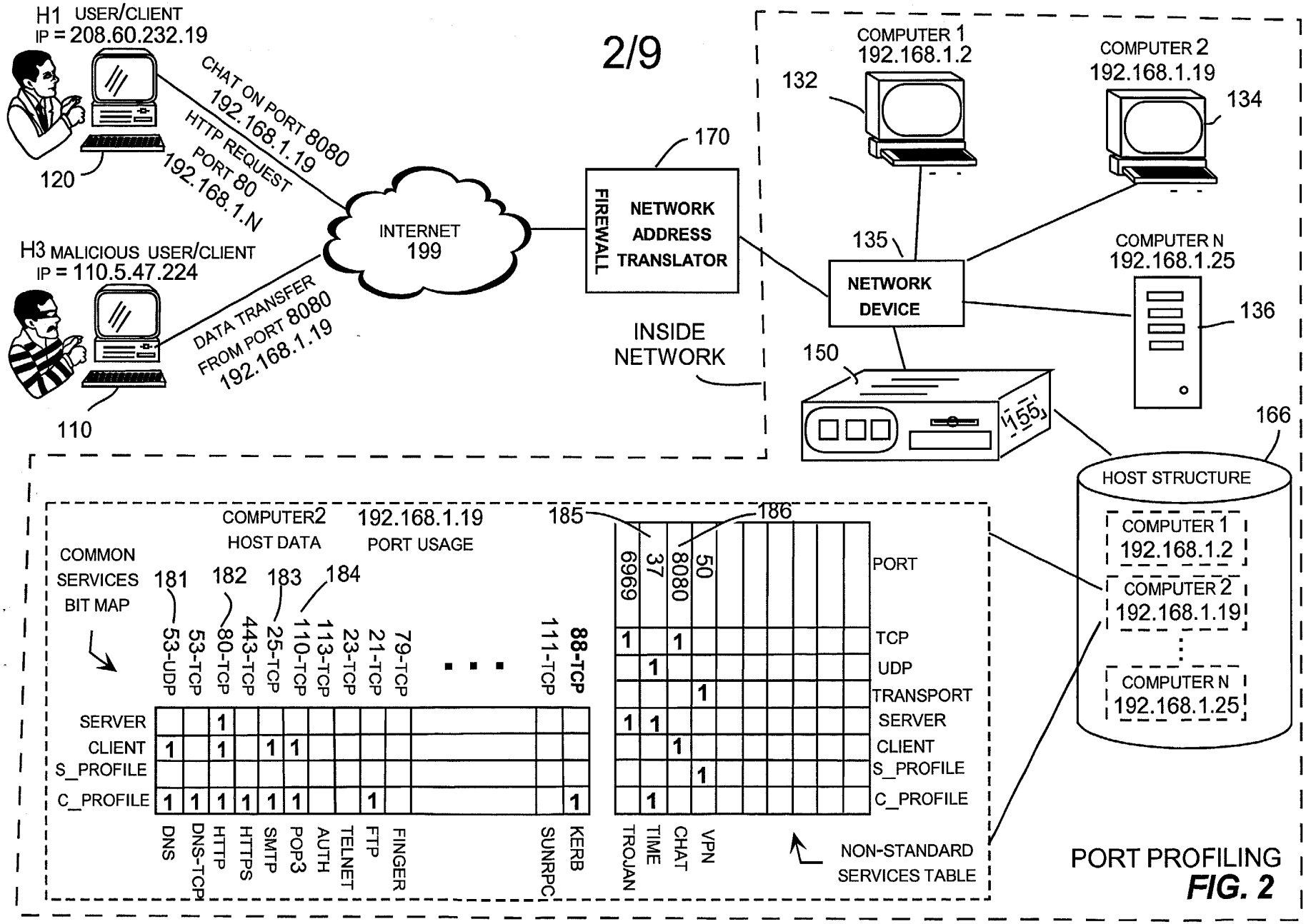


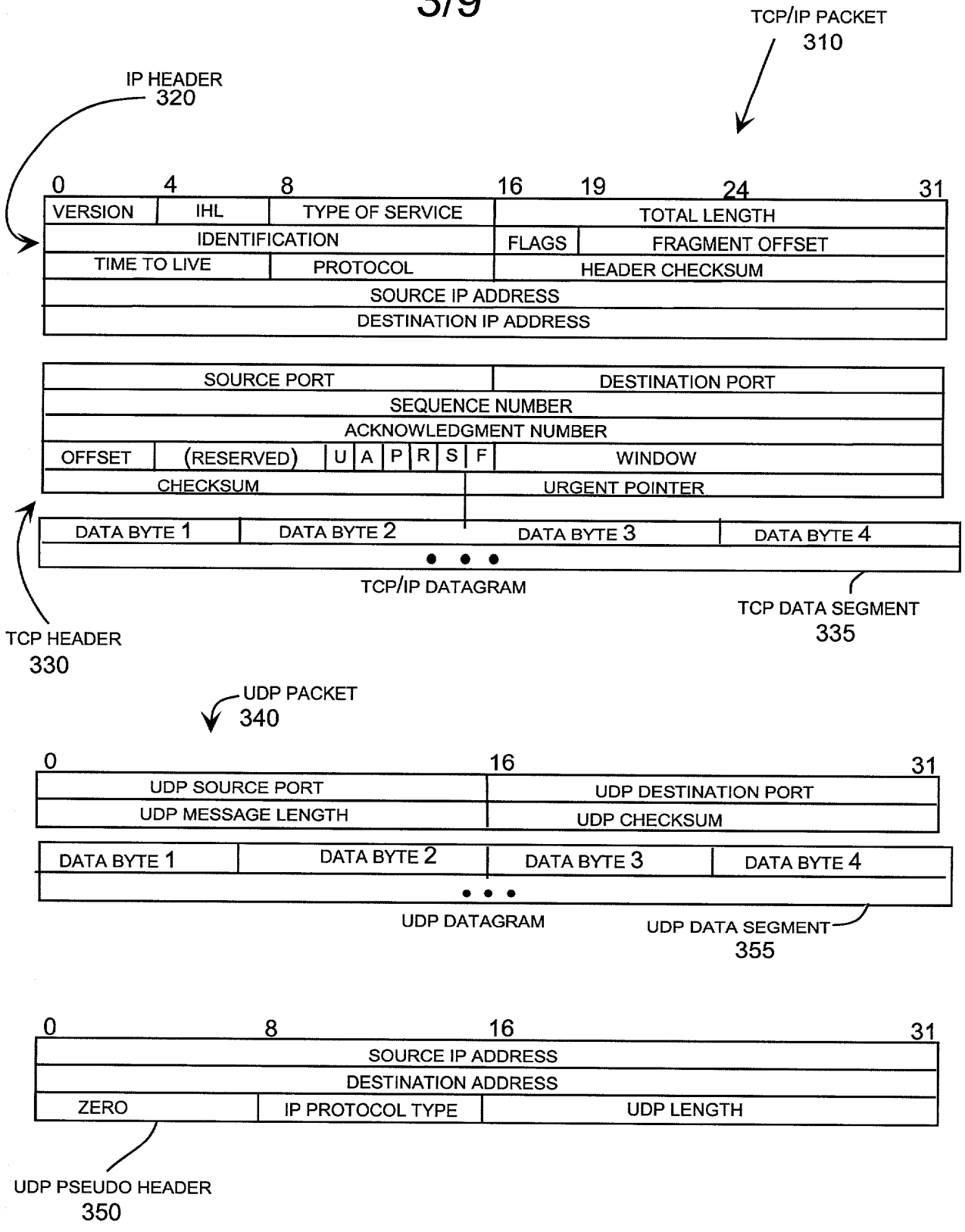
NETWORK DATA COLLECTION

FIG. 1



PORT PROFILING

FIG. 2



PACKET HEADERS

FIG. 3

TCP/IP SESSION
400

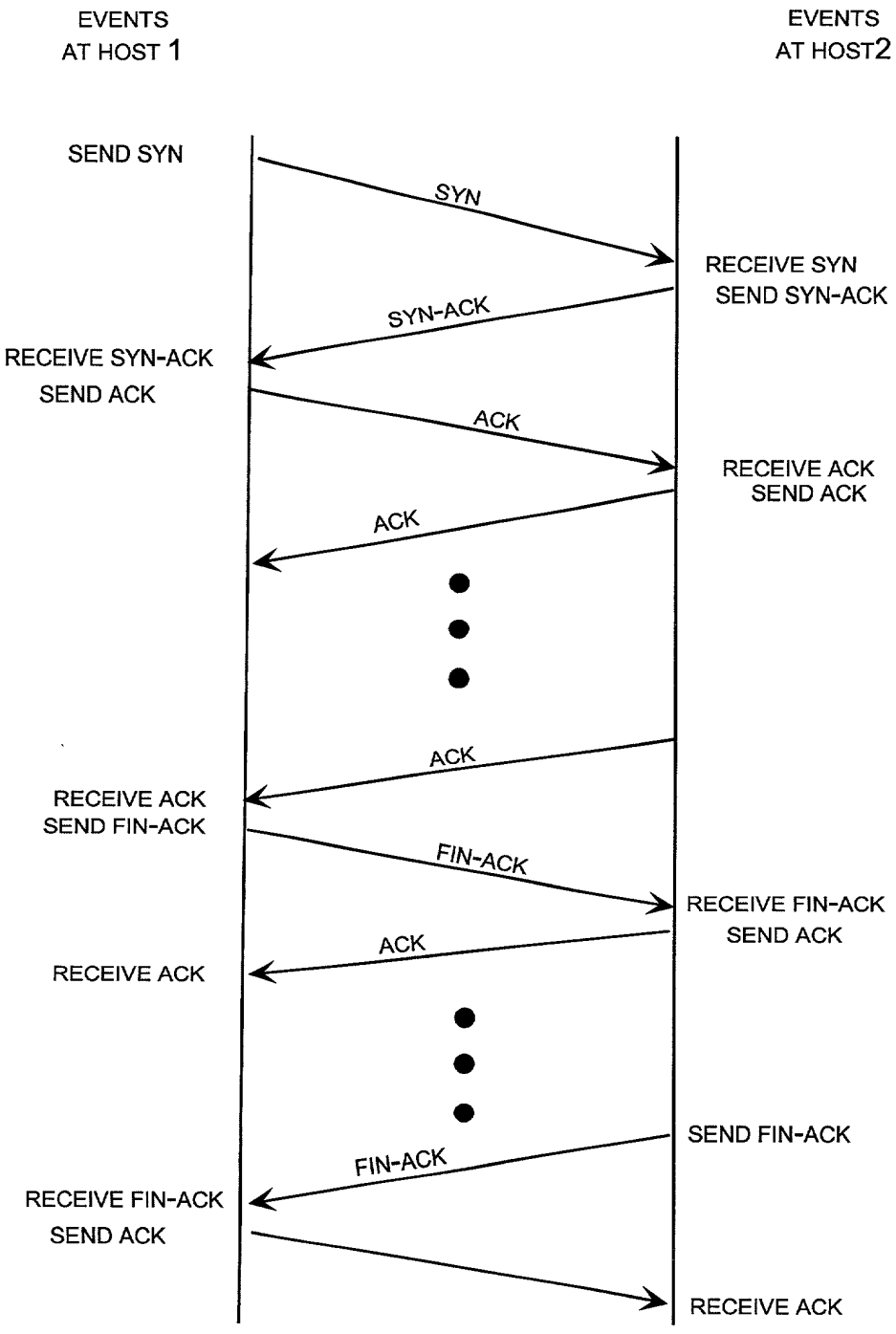


FIG. 4

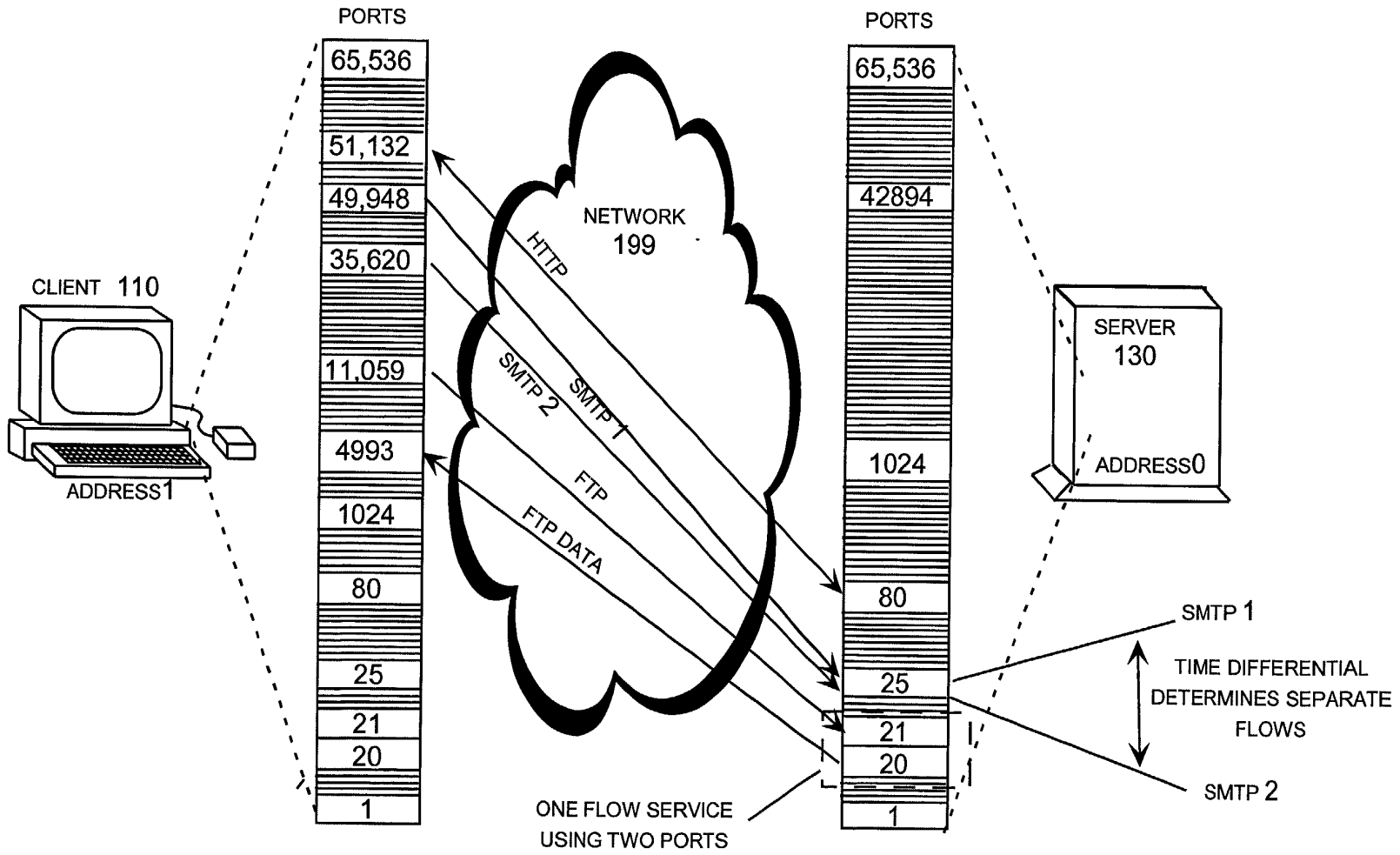
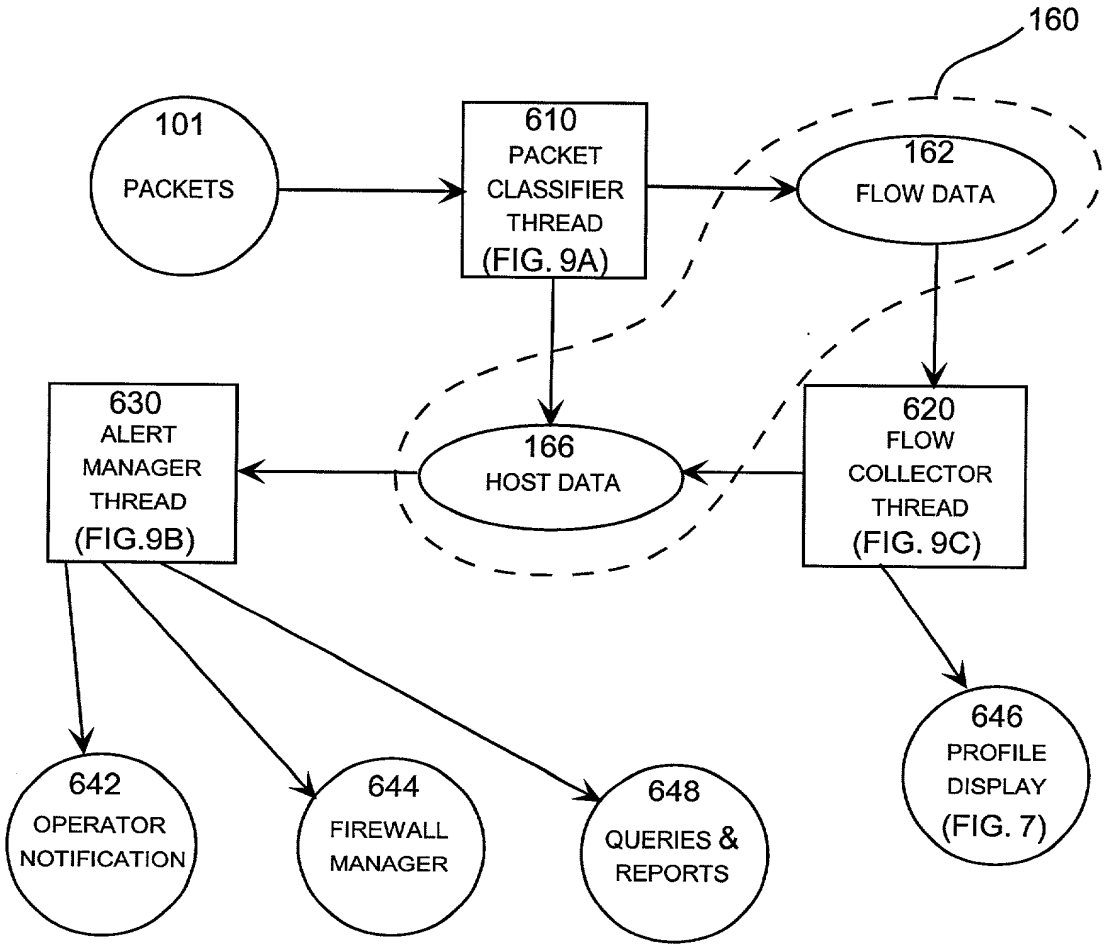

NETWORK SERVICES
PORTS
65,536
51,132
49,948
35,620
11,059
4993
1024
80
25
21
20
1
CLIENT 110
ADDRESS1
NETWORK
199
HTTP
SMTP 2
SMTP 1
FTP
FTP DATA
PORTS
65,536
42894
1024
80
25
21
20
1
SERVER
130
ADDRESS0
SMTP 1
TIME DIFFERENTIAL
DETERMINES SEPARATE
FLOWS
SMTP 2
ONE FLOW SERVICE
USING TWO PORTS

FIG. 5

PORT PROFILING ENGINE
155



PROGRAM THREADS: SQUARES

DATA STRUCTURES: OVALS

DATA INPUT/OUTPUT: CIRCLES

FIG. 6

PROFILE DISPLAY
700

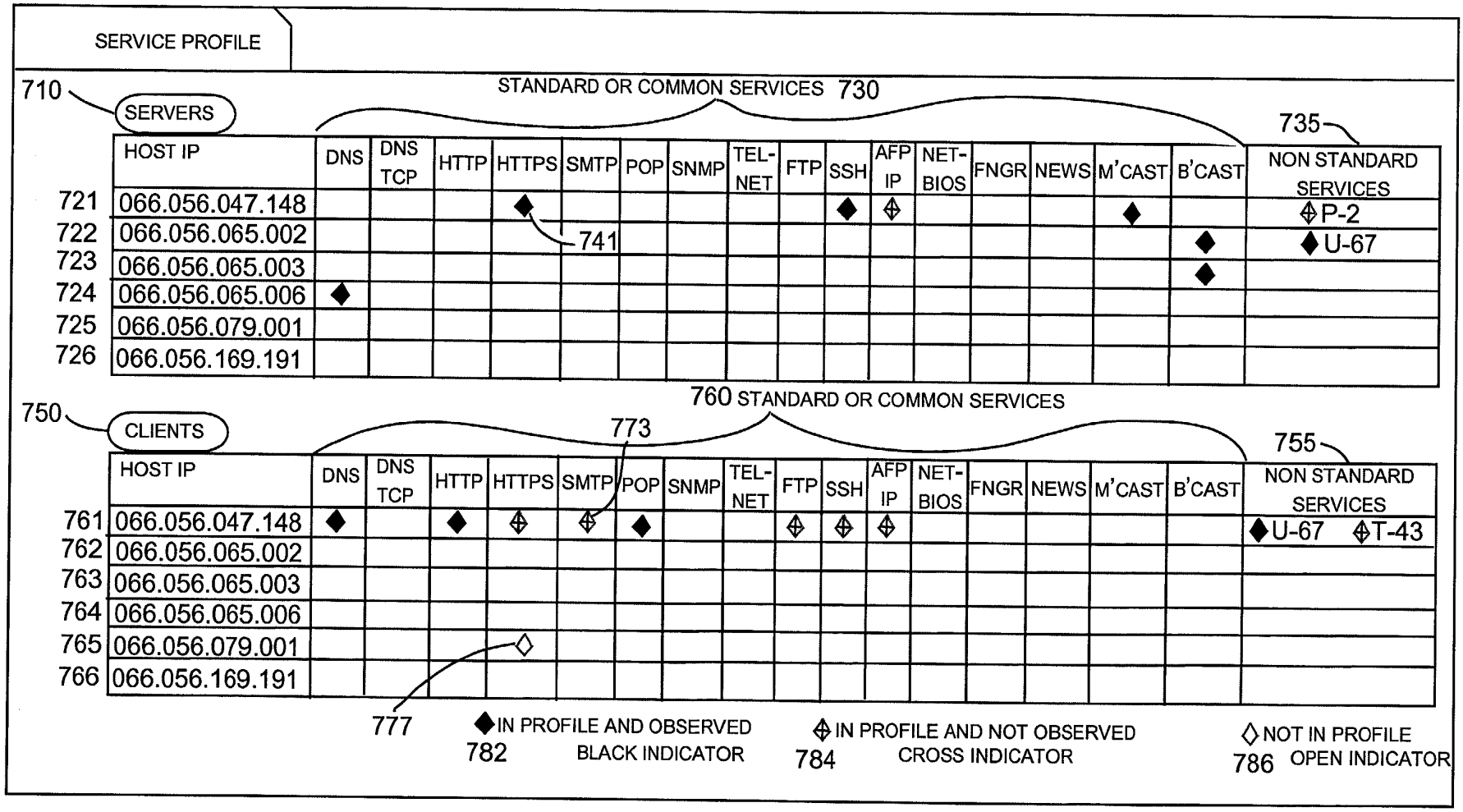


FIG. 7

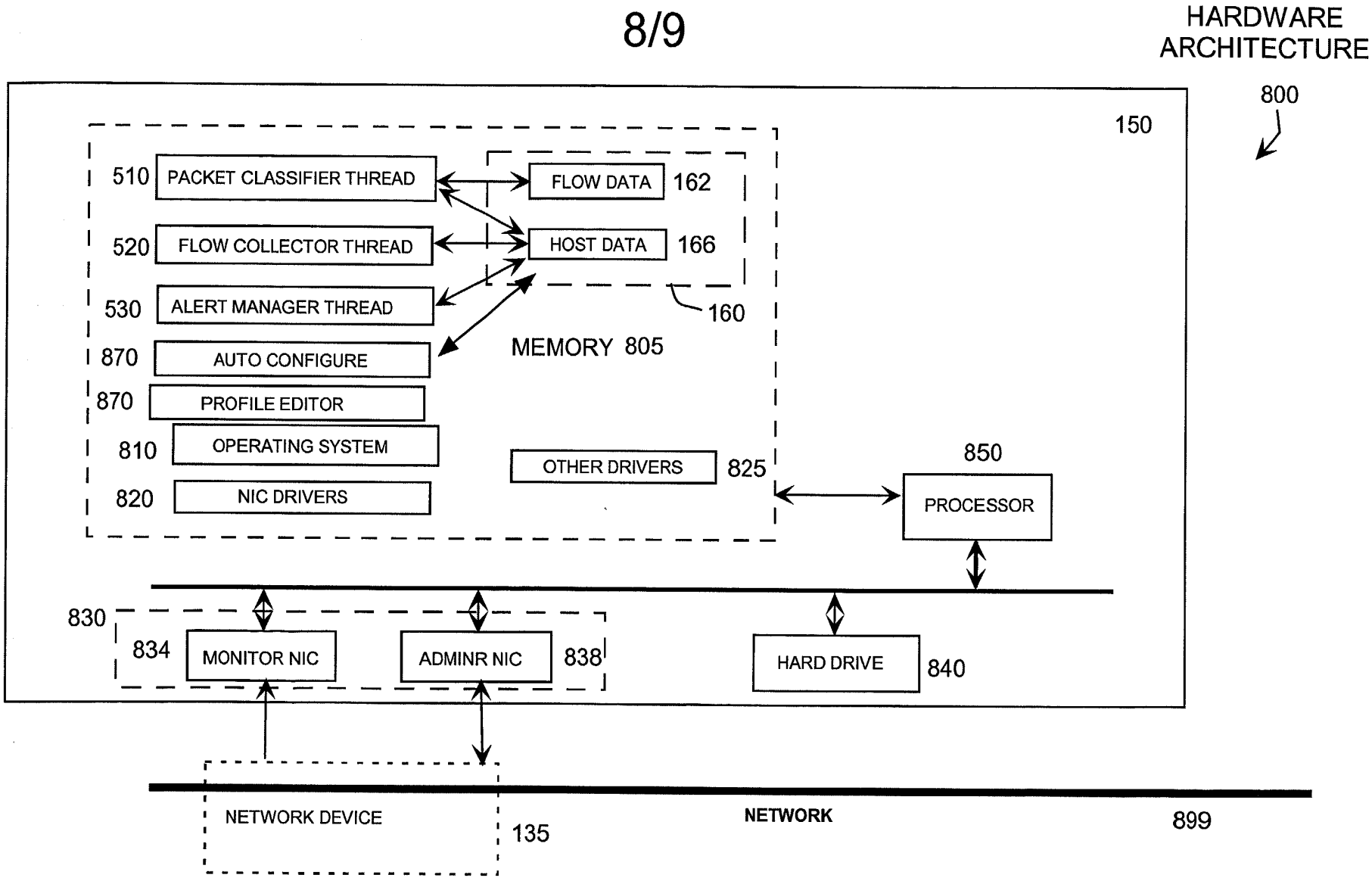

HARDWARE ARCHITECTURE
800
150
510 PACKET CLASSIFIER THREAD
FLOW DATA 162
520 FLOW COLLECTOR THREAD
HOST DATA 166
530 ALERT MANAGER THREAD
160
MEMORY 805
870 AUTO CONFIGURE
870 PROFILE EDITOR
810 OPERATING SYSTEM
820 NIC DRIVERS
OTHER DRIVERS 825
850
PROCESSOR
830
834 MONITOR NIC
ADMINR NIC 838
HARD DRIVE 840
NETWORK DEVICE 135
NETWORK 899

FIG. 8

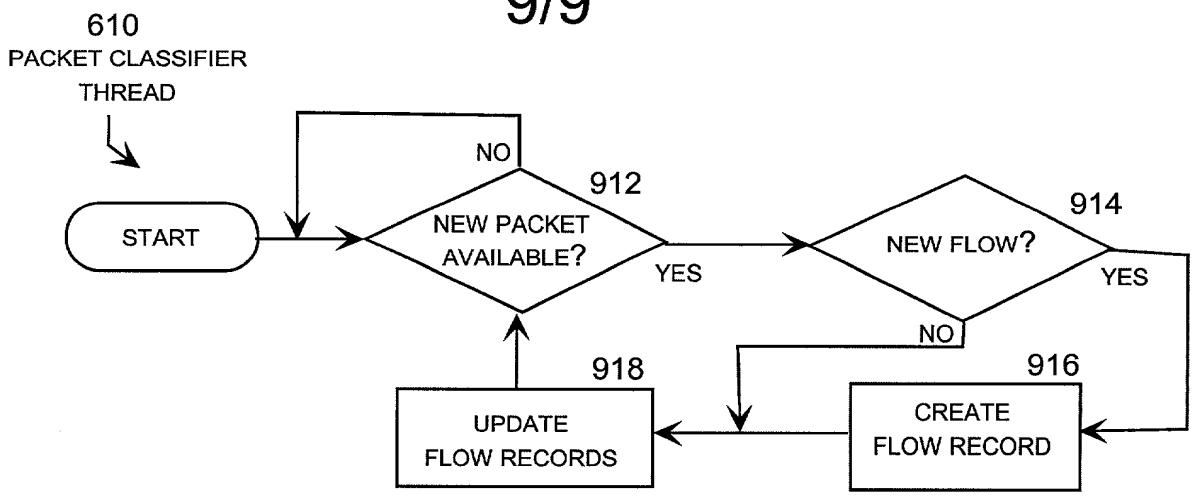


FIG. 9A

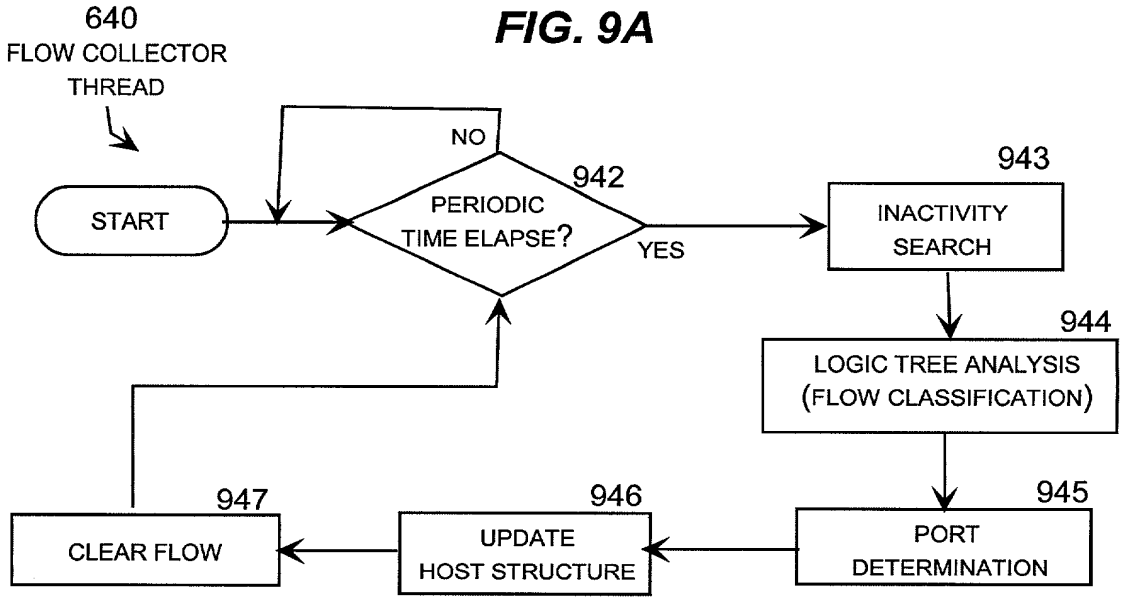


FIG. 9B

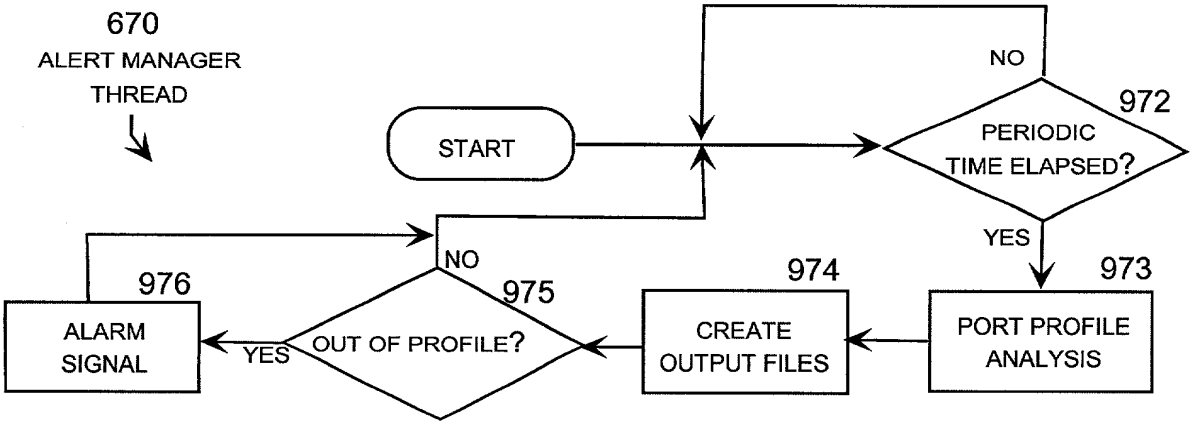


FIG. 9C